IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: KILKKILÄ

Serial No. TO BE ASSIGNED

Corresponding to PCT/FI00/00699, filed August 17, 2000

Filed: January 24, 2002 Docket No.: 602.361USW1

Title: METHOD AND SYSTEM FOR IDENTIFICATION IN A TELECOMMUNICATION SYSTEM

CERTIFICATE UNDER 37 C.F.R. 1.10:
'Express Mail' mailing number: EV017368386US
Date of Deposit: 1/24/02
The undersigned hereby certifies that this Transmittal Letter and the paper or fee, as described herein, are being deposited with the United States Postal Service 'Express Mail Post Office To Addressee' service under 37 CFR 1.10 and is addressed to the Assistant Commissioner for Patents, Washington, D.C. 20231
By: Lee Thao
Lee Thao

PRELIMINARY AMENDMENT

Box Patent Application
Assistant Commissioner for Patents
Washington, D.C. 20231

Dear Sir:

Please enter the following preliminary amendment into the above-referenced application.

ABSTRACT

Please insert the attached abstract into the application as the last page thereof.

CLAIMS

Please amend claims 1-21 as follows. A clean copy of the amended and new claims is included below. A marked up copy of the entire claim set is included in Appendix A.

CLAIMS

1. Method for user identification and ascertainment of authenticity of parties in a telecommunication system comprising:

a telecommunication network;

a source system connected to the telecommunication network;

a target system connected to the telecommunication network;

said method comprising the steps of:

storing user identifiers and associated passwords in the source system and in the target system;

logging on into the source system by entering a user identifier and a password corresponding to it;

identifying the user in the source system;

setting up a remote session to the target system;

wherein the method further comprises the steps of:

generating identical indexed encryption keys in the source system and in the target system;

encrypting the password associated with the user identifier in the source system using the encryption key indicated by a first index, and sending the encrypted data as well as the first index and the user identifier to the target system;

encrypting the password associated with the user identifier in the target system using an encryption key indicated by the index received;

performing a first comparison between the received password and the password encrypted in the target system;

encrypting in the target system the password received from the source system using an encryption key indicated by a second index, and sending the encrypted data and the second index to the source system;

encrypting the encrypted password initially sent from the source system to the target system again using the encryption key indicated by the second index received from the target system;

performing a second comparison between the encrypted password received from the target system and the password encrypted in the source system using the encryption keys indicated by the first and second indexes; and

approving the setup of the remote session if the results of the comparisons are coincident.

2. Method as defined in claim 1, wherein the setup of the remote session is prevented if the results of the first or the second comparison are not coincident.

3. Method as defined in claim 1, wherein separate identification data is generated;

the identification data is encrypted in the source system using the encryption key indicated by the first index and the encrypted data is sent to the target system;

the identification data received from the source system is encrypted in the target system using the encryption key indicated by the second index and the encrypted data as well as the second index are sent back to the source system;

the identification data encrypted using the encryption key indicated by the first index which was initially sent to the target system is encrypted again in the source system using the encryption key indicated by the second index received from the target system;

a third comparison is performed between the encrypted identification data received from the target system and the identification data just encrypted in the source system; and

the setup of the remote session is approved if the result of the comparison is coincident.

4. Method as defined in claim 3, wherein the setup of the remote session is prevented if the result of the third comparison is not coincident.

5. Method as defined in claim 1, wherein

the identification data is sent simultaneously with the user data; or

the identification data is sent in separation from the user data.

6. Method as defined in claim 1, wherein the time data and/or data individualizing the source system is added to the identification data.

7. Method as defined in claim 1, wherein the encryption keys are generated using a certain predetermined algorithm.

8. Method as defined in claim 1, wherein the encryption keys are stored on a special encryption key list.

9. Method as defined in claim 1, wherein the index is generated on a random basis or on the basis of a predetermined algorithm.

10. Method as defined in claim 1, wherein a one-way encryption algorithm is used for the encryption of data in the source system and in the target system.

11. Method as defined in claim 1, wherein the telecommunication system is a telephone exchange system.

12. Method as defined in claim 1, wherein the source system and/or the target system are telephone exchanges.

13. Method as defined in claim 1, wherein the telecommunication network is an operation and maintenance network.

14. System for user identification and ascertainment of authenticity of parties in a telecommunication system comprising:

a telecommunication network;

a source system connected to the telecommunication network;

a target system connected to the telecommunication network;

in which system it is possible to store user identifiers and associated passwords in the source system and in the target system, log on into the source system by entering a user identifier and a password corresponding to it, identify the user in the source system and set up a remote session to the target system;

wherein the system comprises:

means for generating identical indexed encryption keys in the source system and in the target system;

means for encrypting data in the source and target systems using an encryption key indicated by an index;

means for transmitting data between the source and target systems;

means for performing a comparison in the source and target systems;

means for approving the setup of a remote session.

15. System as defined in claim 14, wherein the system comprises means for preventing the setup of a remote session.

16. Method as defined in claim 14, wherein the system comprises means for generating identification data and adding time data and/or data individualizing the source system to the identification data.

17. System as defined in claim 14, wherein the system comprises an encryption key list for the storage of encryption keys.

18. System as defined in claim 14, wherein the system comprises means for generating an index on a random basis or on the basis of a predetermined algorithm.

19. System as defined in claim 14, wherein the telecommunication system is a telephone exchange system.

20. System as defined in claim 14, wherein the source system and/or the target system are telephone exchanges.

21. System as defined in claim 14, wherein the telecommunication network is an operation and maintenance network.

REMARKS

The above preliminary amendment is made to insert an abstract page into the application and to remove multiple dependencies from claims 3, 5-13 and 16-21.

Applicant respectfully requests that this preliminary amendment be entered into the record prior to calculation of the filing fee and prior to examination and consideration of the above-identified application.

If a telephone conference would be helpful in resolving any issues concerning this communication, please contact Applicant's attorney of record, Michael B. Lasky at 952-235-4106.

Respectfully submitted,

Altera Law Group, LLC
6500 City West Parkway, Suite 100
Minneapolis, Minnesota 55344-7701
952-253-4100

Date: 1-24-02

By: _____
Michael B. Lasky
Reg. No. 29,555

MBL/mar/ems

Appendix A
Marked Up Version of Entire Claim Set

CLAIMS

1. Method for user identification and ascertainment of authenticity of parties in a telecommunication system comprising:

a telecommunication network [(OM)];

a source system [(LE1)] connected to the telecommunication network [(OM)];

a target system [(LE2)] connected to the telecommunication network [(OM)];

said method comprising the steps of:

storing user identifiers and associated passwords in the source system [(LE1)] and in the target system [(LE2)];

logging on into the source system [(LE1)] by entering a user identifier and a password corresponding to it;

identifying the user in the source system [(LE1)];

setting up a remote session to the target system [(LE2)];

[characterized in that in that] wherein the method further comprises the steps of:

generating identical indexed encryption keys in the source system [(LE1)] and in the target system [(LE2)];

encrypting the password associated with the user identifier in the source system [(LE1)] using the encryption key indicated by a first index, and sending the encrypted data as well as the first index and the user identifier to the target system [(LE2)];

encrypting the password associated with the user identifier in the target system [(LE2)] using an encryption key indicated by the index received;

performing a first comparison between the received password and the password encrypted in the target system [(LE2)];

encrypting in the target system [(LE2)] the password received from the source system [(LE1)] using an encryption key indicated by a second index, and sending the encrypted data and the second index to the source system [(LE1)];

encrypting the encrypted password initially sent from the source system [(LE1)] to the target system [(LE2)] again using the encryption key indicated by the second index received from the target system [(LE2)];

performing a second comparison between the encrypted password received from the target system [(LE2)] and the password encrypted in the source system [(LE1)] using the encryption keys indicated by the first and second indexes; and

approving the setup of the remote session if the results of the comparisons are coincident.

2. Method as defined in claim 1, [characterized in that] wherein the setup of the remote session is prevented if the results of the first or the second comparison are not coincident.

3. Method as defined in claim 1 [or 2], [characterized in that] wherein separate identification data is generated;

the identification data is encrypted in the source system [(LE1)] using the encryption key indicated by the first index and the encrypted data is sent to the target system [(LE2)];

the identification data received from the source system [(LE1)] is encrypted in the target system [(LE2)] using the encryption key indicated by the second index and

the encrypted data as well as the second index are sent back to the source system [(LE1)];

the identification data encrypted using the encryption key indicated by the first index which was initially sent to the target system [(LE2)] is encrypted again in the source system [(LE1)] using the encryption key indicated by the second index received from the target system [(LE2)];

a third comparison is performed between the encrypted identification data received from the target system [(LE2)] and the identification data just encrypted in the source system [(LE1)]; and

the setup of the remote session is approved if the result of the comparison is coincident.

4. Method as defined in claim 3, [characterized in that] wherein the setup of the remote session is prevented if the result of the third comparison is not coincident.

5. Method as defined in [any one of the preceding claims] claim 1 [- 4], [characterized in that] wherein the identification data is sent simultaneously with the user data; or

the identification data is sent in separation from the user data.

6. Method as defined in [any one of the preceding claims] claim 1 [- 5], [characterized in that] wherein the time data and/or data individualizing the source system is added to the identification data.

7. Method as defined in [any one of the preceding claims] claim 1 [- 6], [characterized in that] wherein the encryption keys are generated using a certain predetermined algorithm.

8. Method as defined in [any one of the preceding claims] claim 1 [- 7], [characterized in that] wherein the encryption keys are stored on a special encryption key list.

9. Method as defined in [any one of the preceding claims] claim 1 [- 8], [characterized in that] wherein the index is generated on a random basis or on the basis of a predetermined algorithm.

10. Method as defined in [any one of the preceding claims] claim 1 [- 9], [characterized in that] wherein a one-way encryption algorithm is used for the encryption of data in the source system [(LE1)] and in the target system [(LE2)].

11. Method as defined in [any one of the preceding claims] claim 1 [- 10], [characterized in that] wherein the telecommunication system is a telephone exchange system.

12. Method as defined in [any one of the preceding claims] claim 1 [- 11], [characterized in that] wherein the source system [(LE1)] and/or the target system [(LE2)] are telephone exchanges.

13. Method as defined in [any one of the preceding claims] claim 1 [- 12], [characterized in that] wherein the telecommunication network [(OM)] is an operation and maintenance network.

14. System for user identification and ascertainment of authenticity of parties in a telecommunication system comprising:

a telecommunication network [(OM)];

a source system [(LE1)] connected to the telecommunication network [(OM)];

a target system [(LE2)] connected to the telecommunication network [(OM)];

in which system it is possible to store user identifiers and associated passwords in the source system [(LE1)] and in the target system [(LE2)], log on into the source system [(LE1)] by entering a user identifier and a password corresponding to it, identify the user in the source system [(LE1)] and set up a remote session to the target system [(LE2)];

[characterized in that] wherein the system comprises:

means [(1)] for generating identical indexed encryption keys in the source system [(LE1)] and in the target system [(LE2)];

means [(2)] for encrypting data in the source and target systems using an encryption key indicated by an index;

means [(3)] for transmitting data between the source and target systems;

means [(4)] for performing a comparison in the source and target systems;

means [(5)] for approving the setup of a remote session.

15. System as defined in claim 14, [characterized in that] wherein the system comprises means [(6)] for preventing the setup of a remote session.

16. Method as defined in claim 14 [or 15], [characterized in that] wherein the system comprises means [(7)] for generating identification data and adding time data and/or data individualizing the source system to the identification data.

17. System as defined in [any one of the preceding claims] claim 14 [- 16], [characterized in that] wherein the system comprises an encryption key list [(8)] for the storage of encryption keys.

18. System as defined in [any one of the preceding claims] claim 14 [- 17], [characterized in that] wherein the system comprises means [(9)] for generating an index on a random basis or on the basis of a predetermined algorithm.

19. System as defined in [any one of the preceding claims] claim 14 [- 18], [characterized in that] wherein the telecommunication system is a telephone exchange system.

20. System as defined in [any one of the preceding claims] claim 14 [- 19], [characterized in that] wherein the source system [(LE1)] and/or the target system [(LE2)] are telephone exchanges.

21. System as defined in [any one of the preceding claims] claim 14 [- 20], [characterized in that] wherein the telecommunication network [(OM)] is an operation and maintenance network.